## REMARKS

In the above-noted Official Action, claims 1-33 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. Claims 1-5, 7-16, 18-27 and 29-33 were rejected under 35 U.S.C. §103(a) over REARDON (U.S. Patent No. 6,212,635) in view of STEIN ("Web Security – A Step-by-Step Reference Guide"). Claims 6, 17 and 28 were rejected under 35 U.S.C. §103(a) over REARDON in view of STEIN, and further in view of ABADI et al. (U.S. Patent No. 5,315,657).

Applicants traverse each of the above-noted rejections. In this regard, upon entry of the present amendment, claims 1-33 will have been cancelled without prejudice to or disclaimer of the subject matter recited therein. Claims 34-66 will have been added for consideration by the Examiner. Claims 34-46 recite combinations of features similar to the combinations of features previously recited in claims 1-33. However, claims 34-66 have been revised to ensure that the features therein are not interpreted as "means plus function" or "steps of" recitations. Claims 34-46 have also been revised to more clearly recite the features of the claimed invention.

Applicants traverse the rejection of claims under 35 U.S.C. §112, first paragraph. In this regard, it appears that the basic objection is the timing recited in the claims. In particular, the Official Action indicates that a user would not be able to store data (i.e., a system security manager's certificate) on a computer unless an operating system has previously been installed on the computer. By the present amendment, claims 34-66 have been revised to eliminate the objected-to features of, e.g., "when installing an operating system on a server computer" in new claims 34, 45 and 56. Applicants respectfully submit that the above-noted amendments do not narrow the scope of the

present claims. In any case, the herein-contained amendments are believed to eliminate the basis for the rejections under 35 U.S.C. §112, first paragraph as lacking enablement. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection under 35 U.S.C. §112, first paragraph.

Applicants traverse each of the rejections under 35 U.S.C. 103(a). In this regard, the invention recited in the pending claims is generally directed to including the certificate of the system security manager and the digital signature verification in the kernel level of the server computer operating system (OS). The computer system can thereby be protected from hacking caused by vulnerabilities in the operating system. These features are described at, for example, page 14, lines 4-17.

In contrast to the invention recited in claims 34-66, REARDON relates to a password based authentication method. In contrast to the assertions in the Official Action, REARDON does not disclose a signature key. Accordingly, REARDON does not disclose or suggest the features related to a signature as recited in claims 34-66.

In particular, columns 7 and 8 of REARDON only disclose that the "system security manager" is assigned a single master configuration key "U.0" (see co. 8, lines 7-14), and not "keys" as recited in new claim 34. In this regard, the key pair "SG.1" at col. 7, lines 56-60 of REARDON is "[t]he security gateway's own key pair", and not a pair assigned to the system security manager. As disclosed at col. 10, lines 40-59, SG.1 is created using a hash or checksum of random data of the user, but is assigned as a unique key pair for the security gateway of a computer system. Accordingly, SG.1 is not a "system security manager's digital signature keys" as recited in new claim 34.

Additionally, the outstanding Official Action incorrectly asserts, at page 4, that a "security gateway... meets the limitation of a security kernel". A security gateway in REARDON is not an inner constituent of an operating system. Rather, a security gateway in REARDON is a hardware component separate from the operating system (see Abstract, lines 10-15), a programmable device independent of a CPU (see col. 7, lines 1-7), and is operated cooperatively with a security program to encrypt the private key (see col. 16, lines 36-45 and col. 30, lines 19-24).

Furthermore, the Official Action admits that REARDON does not disclose storing a key together with a corresponding certificate onto a security kernel. However, the Official Action takes Official Notice that the claimed limitations would be met, and mischaracterizes these features as merely "storing a private key together with the corresponding certificate". However, Official Notice may only be taken where the asserted teachings are so well known in the art as to be subject to instant recognition, and the claimed combination which includes "storing a system security manager's certificate onto a security kernel on a server computer" is not evidenced in the references applied in the Official Action. Accordingly, Applicants respectfully request, if the taking of Official Notice in the above-noted manner is maintained, that the Examiner provide citation to a reference that discloses or suggests the above-noted feature recited in Applicants' claims.

Moreover, the method taught in REARDON has vulnerabilities. In particular REARDON encrypts private keys of all users, such as U.0R, U.1R, and U.XR... using SG.1B (public key of the security gateway's own key pair) and stores the encrypted private keys. However, if SG.1R (private key of the security gateway's own key pair) is

exposed (or drained), the private keys U.0R, U.1R and U.XR of all users are exposed, which renders the method of REARDON unsafe and unstable. As a result, the method of REARDON can be defeated by decrypting the contents of all files that are encrypted by users. Moreover, the intruder can masquerade identification of users and forge important information that is fundamental to a system security such as an access authority.

Further, using REARDON's own definition of a "digital certificate" at col. 6, lines 9-39, REARDON would not store a system security manager's certificate onto a security kernel with a digital key. Rather, at col. 10, lines 56-59, the key pair SG.1 assigned to the gateway is created using data provided by the installer. Thus, SG.1 is not a system security manager's key pair, let alone digital certificate, and there is no teaching in REARDON that a certifying authority would issue a digital certificate for the user's data to certify the user in the user's own system.

There is additionally not any motivation to modify REARDON to provide the above-noted limitations. In any case, the above-noted shortcomings of REARDON are not remedied by STEIN. Rather, STEIN relates to an SSL protocol based on a signature-based authentication method using a digital certificate. However, STEIN discloses a method of issuing, managing, authenticating and encrypting a client certificate at an application program layer to apply the digital certificate to Web security (see p. 293, lines 1-12). In particular, STEIN makes it possible for a plurality of clients trying to access a network through a Web server based on internet, e-mail etc... to mutually authenticate and securely communicate.

However, the SSL protocol of STEIN is operated in the application layer by clients on the Web. Accordingly, STEIN does not disclose or suggest features relating to including the certificate of the system security manager and the digital signature verification in the kernel level of the server computer operating system (OS). In particular, STEIN does not disclose or suggest operating in the kernel layer of the server computer operating system, and therefore does not provide the claimed method of protecting the server computer operating system.

ABADI also does not disclose or suggest the above-noted features recited in Applicants' claims. In this regard, ABADI provides a security method in a distributed system using a global naming system (GNS) and access control lists (ACL). However, ABADI is also not related to operating in the kernel layer of the server computer operating system.

As described above, the claims of the present invention constitute the security kernel based on the signature-based authentication in the server computer operating system. In contrast, the references relied-upon in the outstanding Official Action do not address or overcome the problem of a security system with conventional password-based authentication implemented in an application program, user or network level. The problems addressed and overcome by the invention recited in Applicants' claims is described at page 2, lines 3-6 of the present application.

Therefore, the present invention has a different object than the references applied in the outstanding Official Action, which each use conventional password-based authentication or Web-based authentication. Accordingly, the invention recited in Applicants' claims provides a stable computer system that is safe against attacks

directed to operating system vulnerabilities. In particular, there is no teaching in the applied references, whether considered alone or in any proper combination, that would provide the benefits of the invention recited in Applicants' claims.

Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the outstanding rejections.

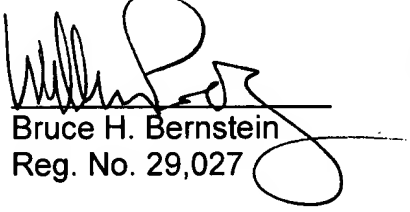
## SUMMARY AND CONCLUSION

Applicant believes that the present application is in condition for allowance, and respectfully requests an indication to that effect. Applicant has discussed the features recited in Applicant's claims and has shown that these features are not taught, disclosed or rendered obvious by the references cited by the Examiner. Applicant has amended the claims to clarify the features recited therein. Accordingly, reconsideration of the outstanding Official Action and allowance of the present application and all the recited claims therein are respectfully requested and now believed to be appropriate

Any amendments to existing claims which have been made in this amendment, and which have not been specifically noted to overcome a rejection based upon the prior art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

Should the Examiner have any questions, please contact the undersigned at the telephone number provided below.

Respectfully submitted,
You-Jin EUN et al.



William Pieprz
Reg. No. 33,630

Bruce H. Bernstein
Reg. No. 29,027

November 8, 2005
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191